IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

AUTH TOKEN LLC, Plaintiff, v. **TOTAL SYSTEM SERVICES LLC,** Defendant.	Civil Action No.: 1:23-cv-00169 **TRIAL BY JURY DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

1. Plaintiff Auth Token LLC ("Plaintiff"), through its attorneys, complains of Total System Services LLC ("Defendant"), and alleges the following:

PARTIES

2. Plaintiff Auth Token LLC is a corporation organized and existing under the laws of Delaware that can receive mail at 261 West 35th Street – Suite 1003, New York, New York 10001.

3. Defendant Total System Services LLC is a limited liability company organized and existing under the laws of Delaware that maintains an established place of business at One TSYS Way, Columbus, Georgia 31901.

4. Upon information and belief, Defendant is a subsidiary of Global Payments, Inc., which owns and/or operates a place of business in this District located at 21320 Hillsdale Avenue, Cleveland, Ohio 44126.

5. Upon information and belief, Defendant is registered to do business in this District and may be served via its Registered Agent c/o CT Corporation System, 4400 Easton Commons Way – Suite 125, Columbus, Ohio 43219.

JURISDICTION

6. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

7. This Court has exclusive subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has personal jurisdiction over Defendant because it has engaged in systematic and continuous business activities in this District and has an established place of business in this District. As described below, Defendant has committed acts of patent infringement giving rise to this action within this District.

VENUE

9. Venue is proper in this District under 28 U.S.C. § 1400(b) because Defendant has an established place of business in this District. In addition, Defendant has committed acts of patent infringement in this District, and Plaintiff has suffered harm in this district.

PATENTS-IN-SUIT

10. Plaintiff is the assignee of all right, title and interest in United States Patent Nos. 8,375,212 (the "'212 Patent"); and 8,688,990 (the "'990 Patent") (collectively the "Patents-in-Suit"); including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the Patents-in-Suit. Accordingly, Plaintiff possesses the exclusive right and standing to prosecute the present action for infringement of the Patents-in-Suit by Defendant.

THE '212 PATENT

11. The '212 Patent is entitled "Method for personalizing an authentication token," and issued 2013-02-12. The application leading to the '212 Patent was filed on 2010-12-27. A true and correct copy of the '212 Patent is attached hereto as Exhibit 1 and incorporated herein by reference.

12. Plaintiff is presently the owner of the '212 Patent, having received all right, title and interest in and to the '212 Patent from the previous assignee of record. Plaintiff possesses all rights of recovery under the '212 Patent, including the exclusive right to recover for past infringement.

13. To the extent required, Plaintiff has complied with all marking requirements under 35 U.S.C. § 287 with respect to the '212 Patent.

14. One claimed inventions in the '212 Patent pertains to an authentication token using a smart card. Ex.1 at Col.1:13-14.

15. As identified in the '212 Patent, prior art systems had technological faults. See Ex. 1 at Col.1:16-Col. 4:10.

16. Prior art systems were familiar with the authentication of remote users in order to enforce secure access control. Ex. 1 at Col. 1:16-17.

17. However, prior art failed to provide personalized authentication in a multi-party environment. The increase in smart-card computing capabilities created new risk for organizations as applications could then be loaded into a smart-card's Electrically Erasable Programmable Read Only Memory (EEPROM) *after* manufacture (i.e. they can be subsequently removed or replaced allowing upgraded applications to be delivered onto the smart cards even after they have been issued to end users). See Ex. 1 at Col. 3:37-45.

18. The ability to have the cards personalized after issuance, lead to an increase in the need to remotely personalize the authentication in a manner that is secure and not at risk for third party interference.

19. Prior art systems and methods ranged from single factor authentication (such as use of a password) to multiple factor authentication (such as use of a physical token in conjunction with a Personal Identification Number (PIN)). See Ex. 1 at Col. 1:18-21.

20. Prior art also identified a variety of tokens that can fulfill the role of the second factor ('something you have'). One exemplary approach was a method of having a series of password each of which can only be used once. See Ex. 1 at Col. 2:27-29.

21. This process used a cryptographic process to generate a one-time password dynamically when it is needed. See Ex. 1 at Col. 2:34-36.

22. Additionally, Smart cards, at the time of invention were in use for a variety of purposes including financial products. See Ex. 1 at Col. 2:49-50.

23. However, they had limited processing capabilities. See Ex. 1 at Col. 2:66-Col. 3:4.

24. As of the '212 Patent's priority date, the newest smartcards were EMV (credit/debit card functionality defined jointly by Europay/Mastercard/Visa) cards that took advantage of improved capabilities to provide better security features. See Ex. 1 at Col. 3:5-9.

25. Subsequently, multi-application smart card operating systems were developed, requiring only the operating system itself to be hardwired into a smart-card's Read Only Memory (ROM). See Ex. 1 at Col. 3:10-13.

26. Because of this new environment, applications can now be loaded into a smart-card's EEPROM after manufacture and they can be removed or replaced even after they have been issued to end users. See Ex. 1 at Col. 3:37-45.

27. In sum, the technological advances in smart-card processing ability, resulted in a computer-centric or network-centric problem (or opportunity) related to an organization's ability to authenticate remote users and provide continued secure access control in a multi-party environment in a personalized manner *after issuance*. As noted during the prosecution of the '212 Patent, prior art did not teach or provide for the ability to lock the authentication token, thereby reducing the risk of third party removing or replacing the personalized authentication.

28. Claim 1 of the '212 Patent is a practical application and inventive step of technology that address these aforementioned specific computer-centric problems associated with computer-centric or network-centric problem (or opportunity) related to an organization's ability to authenticate remote users and provide continued secure access control in a multi-party environment in a personalized manner *after issuance*. As noted during the prosecution of the '212 Patent, prior art did not teach or provide for the ability to lock the authentication token, thereby reducing the risk of third party removing or replacing the personalized authentication.

29. Claim 1 of the '212 Patent states:

> "1. A method for personalizing an authentication token comprising:
> entering by the authentication token into personalization mode;
> requesting from the authentication token, by a personalization device in communication with the authentication token, a serial number of the authentication token;
> encrypting by the personalization device the serial number using a personalization key, and forwarding the encrypted serial number to the authentication token from the personalization device;
> decrypting by the authentication token of the encrypted serial number, and validating by the authentication token that the personalization key is correct;
> establishing an encrypted session between the authentication token and the personalization device using a trans port key:

> sending to the authentication token, by the personalization device, an initial seed value and an initial Secret key using the transport key to encrypt the initial seed value and the initial secret key, the initial seed value and the initial Secret key for facilitating an initial interaction between the authentication token and an interface device; and
>
> storing by the authentication token the initial seed value and the initial secret key after decryption thereof by the authentication token using the transport key, wherein, once the authentication token is personalized with the initial seed value and the initial secret key, the authentication token can no longer enter the personalization mode. Ex. 1 at Col.10:66 – Col. 12:7.

30. Specifically, Claim 1 of the '212 Patent provides a solution to the previous network-centric or internet-centric problems inasmuch as it provides for more robust authentication where, regardless of the smartcard used, the application is personalized to ensure the correct data is stored on the card's EEPROM along with an initial unique consumer code. See Ex. 1 at Col. 5:52-55.

31. Once personalized, "the authentication token can no longer enter the personalization mode." See Ex. 1 at Col. 12:6-7.

32. The specific elements of claim 1, as combined, accomplish the desired result of improve functionality in smartcard security and personalization. *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018) (holding that improving computer security can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem). See also *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018); *Core Wireless Licensing v. LG Elecs., Inc*., 880 F.3d 1356 (Fed. Cir. 2018); *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018); *Uniloc USA, Inc. v. LG Electronics USA*, Inc., 957 F.3d 1303 (Fed. Cir. April 30, 2020).

33. Claim 1 of the '212 Patent provides meaningful details on how to implement its system, and thus adds something inventive.

34. Importantly, during the prosecution of the '212 patent, Claim 1 was allowed after the applicant amended the claims to include specific limitations relating to the personalization modes and their ordered operation. See Exhibit 2, '212 Notice of Allowance at Page 6 and Applicant's Amendment at Pages 18-19.

35. Specifically, Claim 1 of '212 patent was allowed with a limitation that "once the authentication token is personalized with the initial seed value and the initial secret key, the authentication token can no longer enter the personalization mode. *Id.*

36. Thus, the "how to implement" the system of Claim 1 of the '212 Patent corresponds to the USPTO's reasons for allowance. "How" the system operates in an inventive way is the additional security provided for a multi-party environment wherein Claim 1 specifically requires that once the authentication token is personalized with the initial seed value and the initial secret key, the authentication token can no longer enter the personalization mode. *Id*.

37. Claims need not articulate the advantages of the claimed combinations to be eligible. *Uniloc USA, Inc. v. LG Elecs. USA, Inc*., 957 F.3d 1303, 1309 (Fed. Cir. 2020).

38. These specific elements of Claim 1 of the '212 Patent were an unconventional arrangement of elements. *Cellspin Soft, Inc. v. FitBit, Inc.*, 927 F.3d 1306 (Fed. Cir. 2019).

39. Further, regarding the specific non-conventional and non-generic arrangements of known, conventional pieces to overcome an existing problem, the system of Claim 1 in the '212 Patent provides a system that would not preempt all ways of improving security in a multi-party environment. *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016); See also *DDR Holdings, LLC v. Hotels.com, L.P*., 773 F.3d 1245 (Fed. Cir. 2014).

40. Based on the allegations, it must be accepted as true at this stage, that Claim 1 of the '212 Patent recites a specific, plausibly inventive computer implemented system for

authenticating remote users and providing continued secure access control in a multi-party environment in a personalized manner *after the issuance of a smart card*. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019), cert. denied sub nom. *Garmin USA, Inc. v. Cellspin Soft, Inc.*, 140 S. Ct. 907, 205 L. Ed. 2d 459 (2020).

41. Alternatively, there is at least a question of fact that must survive the pleading stage as to whether these specific elements of Claim 1 of the '212 Patent were an unconventional arrangement of elements. *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121 (Fed. Cir. 2018) See also *Berkheimer v. HP Inc*., 881 F.3d 1360 (Fed. Cir. 2018), cert. denied, 140 S. Ct. 911, 205 L. Ed. 2d 454 (2020).

THE '990 PATENT

42. On April 1, 2014 the United States Patent and Trademark Office ("USPTO") duly and legally issued the '990 Patent, entitled "Method for personalizing an authentication token" after a full and fair examination. The application leading to the '990 Patent was filed on February 12, 2013. The '990 Patent is attached hereto as Exhibit 3 and incorporated herein as if fully rewritten.

43. Plaintiff is presently the owner of the '990 Patent, having received all right, title and interest in and to the '990 Patent from the previous assignee of record. Plaintiff possesses all rights of recovery under the '990 Patent, including the exclusive right to recover for past infringement.

44. To the extent required, Plaintiff has complied with all marking requirements under 35 U.S.C. § 287 with respect to the '990 Patent.

45. The '990 Patent shares the same specification as the '212 Patent.

46. The ‘990 Patent sought to overcome the same problems discussed above with respect to the ‘212 Patent.

47. One claimed inventions in the ‘212 Patent pertains to an authentication token using a smart card. Ex.3 at Col.1:16-17.

48. Claim 1 of the ‘990 Patent states:

> “1. A system for personalizing an authentication token comprising:
>
> an interface device, the authentication token, and a personalization device, the system configured to establish an encrypted session between the authentication token and the personalization device using a transport key:
>
> the interface device including a processor, a user interface, and an interface for communication with the authentication token;
>
> the authentication token including a personalization mode, and having a serial number, and the personalization device being configured to encrypt the Serial number of the authentication token using a personalization key, and being configured to forward the encrypted serial number to the authentication token;
>
> the authentication token, when in the personalization mode, being configured to:
>
> receive, from the personalization device, a request for the serial number, and return the serial number to the personalization device:
>
> decrypt the encrypted serial number forwarded from the personalization device, and validate that the personalization key is correct;
>
> receive, from said personalization device through the encrypted session, an initial seed value and initial secret key, the initial seed value and the initial secret key being configured to facilitate an initial interaction between the authentication token and the interface device; and
>
> store the initial seed value and the initial secret key after decryption thereof using the transport key:
>
> wherein, once said authentication token is personalized with the initial seed value and the initial secret key, the authentication token is configured to be unable to again

enter to the personalization mode. Ex. 3 at Col.11:4 – Col.12:12.

49. Claim 1 of the '990 Patent is a practical application and inventive step of technology that address these aforementioned specific computer-centric problems associated with computer-centric problems associated with computer-centric or network-centric problem (or opportunity) related to an organization's ability to authenticate remote users and provide continued secure access control in a multi-party environment in a personalized manner *after issuance*. As noted during the prosecution of the '212 Patent, prior art did not teach or provide for the ability to lock the authentication token, thereby reducing the risk of third party removing or replacing the personalized authentication.

50. Specifically, Claim 1 in the '990 Patent requires: (1) an interface device, the authentication token, and a personalization device; (2) the system configured to establish an encrypted session between the authentication token and the personalization device using a transport key; (3) the interface device including a processor, a user interface, and an interface for communication with the authentication token (4) the authentication token including a personalization mode, and having a serial number (5)the personalization device being configured to encrypt the Serial number of the authentication token using a personalization key, and being configured to forward the encrypted serial number to the authentication token (6) the authentication token, when in the personalization mode, being configured to: receive, from the personalization device, a request for the serial number, and return the serial number to the personalization device: decrypt the encrypted serial number forwarded from the personalization device, and validate that the personalization key is correct (7) receive, from said personalization device through the encrypted session, an initial seed value and initial secret key, the initial seed value and the initial secret key being configured to facilitate an initial interaction between the

authentication token and the interface device; (8) and store the initial seed value and the initial secret key after decryption thereof using the transport key: wherein, once said authentication token is personalized with the initial seed value and the initial secret key, the authentication token is configured to be unable to again enter to the personalization mode. Ex. 3 at Col.11:4 – Col.12:12.

51. These specific elements of Claim 1, as combined, accomplish the desired result of improve functionality in smartcard security and personalization. *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018) (holding that improving computer security can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem). See also *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018); *Core Wireless Licensing v. LG Elecs., Inc*., 880 F.3d 1356 (Fed. Cir. 2018); *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018); *Uniloc USA, Inc. v. LG Electronics USA, Inc.*, 957 F.3d 1303 (Fed. Cir. April 30, 2020).

52. Claim 1 of the '990 Patent provides meaningful details on how to implement its system, and thus adds something inventive.

53. Namely, the USPTO indicated in its Notice of Allowance that the prior art does not disclose or "anticipate the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C. § 102 or § 103 would be proper." See Exhibit 4, '990 Patent Notice of Allowance at pages 8-9.

54. Claims need not articulate the advantages of the claimed combinations to be eligible. *Uniloc USA, Inc. v. LG Elecs. USA, Inc*., 957 F.3d 1303, 1309 (Fed. Cir. 2020).

55. These specific elements of Claim 1 of the '990 Patent were an unconventional arrangement of elements. *Cellspin Soft, Inc. v. FitBit, Inc.*, 927 F.3d 1306 (Fed. Cir. 2019).

56. Further, regarding the specific non-conventional and non-generic arrangements of known, conventional pieces to overcome an existing problem, the system of Claim 1 in the '990 Patent provides a system that would not preempt all ways of improving security in a multi-party environment. *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016); See also *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014).

57. Based on the allegations, it must be accepted as true at this stage, that Claim 1 of the '990 Patent recites a specific, plausibly inventive computer implemented system for authenticating remote users and providing continued secure access control in a multi-party environment in a personalized manner *after the issuance of a smart card*. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019), cert. denied sub nom. *Garmin USA, Inc. v. Cellspin Soft, Inc*., 140 S. Ct. 907, 205 L. Ed. 2d 459 (2020).

58. Alternatively, there is at least a question of fact that must survive the pleading stage as to whether these specific elements of Claim 1 of the '990 Patent were an unconventional arrangement of elements. *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121 (Fed. Cir. 2018) See also *Berkheimer v. HP Inc*., 881 F.3d 1360 (Fed. Cir. 2018), cert. denied, 140 S. Ct. 911, 205 L. Ed. 2d 454 (2020).

COUNT 1: DIRECT INFRINGEMENT OF THE '212 PATENT

59. Plaintiff incorporates paragraphs 1-39, herein by reference.

60. Upon information and belief, Defendant is a vendor of financial products and services.

61. Defendant has directly infringed one or more claims of the '212 Patent in at least this District by making, using, offering to sell, selling and/or importing, without limitation, at least the Defendant products identified in the charts incorporated into this Count below (among the

"Exemplary Defendant Products") that were made in a way that infringes at least the exemplary claims of the '212 Patent, such as Claim 1, also identified in the charts incorporated into this Count below (the "Exemplary '212 Patent Claims") literally or by the doctrine of equivalents.

62. On information and belief, numerous other devices or systems the perform a method that infringed the claims of the '212 Patent have been made, used, sold, imported, and offered for sale by Defendant and/or its customers.

63. Defendant also has directly infringed, literally or under the doctrine of equivalents, the Exemplary '212 Patent Claims, by having its employees internally test and use the methods associated with these Exemplary Products.

64. Upon information and belief, Defendant had knowledge of the infringement, given its relationship as the vendor of the instrumentality to accomplish the method of Claim 1 of the '212 Patent to customers.

65. On information and belief, Defendant sold the Exemplary Defendant Products and distribute product literature and website materials inducing end users and others to use its products in the customary and intended manner that infringed the '212 Patent. See Exhibit 5 (extensively referencing these materials to demonstrate how Defendant has created the Exemplary Defendant Products in a manner that infringed Claim 1 of the '212 Patent).

COUNT 2: DIRECT INFRINGEMENT OF THE '990 PATENT

66. Plaintiff incorporates paragraphs 1-8 and paragraphs 40-56 herein by reference.

67. Defendant has directly infringed one or more claims of the '990 Patent in at least this District by making, using, offering to sell, selling and/or importing, without limitation, at least the Defendant products identified in the charts incorporated into this Count below (among the "Exemplary Defendant Products") that infringe at least the exemplary claims of the '990 Patent

also identified in the charts incorporated into this Count below (the "Exemplary '990 Patent Claims") literally or by the doctrine of equivalents. On information and belief, numerous other devices that infringed the claims of the '990 Patent have been made, used, sold, imported, and offered for sale by Defendant and/or its customers.

68. Defendant also directly infringed, literally or under the doctrine of equivalents, the Exemplary '990 Patent Claims, by having its employees internally test and use a system to effectuate the Exemplary Products.

69. Upon information and belief, Defendant had knowledge of the infringement given its relationship as a vendor of the instrumentality to provide the system of Claim 1 of the '990 Patent to customers.

70. On information and belief, Defendant sold the Exemplary Defendant Products and distribute product literature and website materials inducing end users and others to use its products in the customary and intended manner that was made with a system that infringes the '990 Patent. See Exhibit 6.

JURY DEMAND

71. Under Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff respectfully requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. A judgment that the '212 Patent is valid and enforceable;

B. A judgment that Defendant has infringed directly one or more claims of the '212 Patent;

C. A judgment that the '990 Patent is valid and enforceable;

D. A judgment that Defendant has infringed directly and indirectly one or more claims of the ’990 Patent;

E. An accounting of all damages not presented at trial;

F. A judgment that awards Plaintiff all appropriate damages under 35 U.S.C. § 284 for Defendant's continuing or future infringement, up until the date such judgment is entered with respect to the Patents-in-Suit, including pre- or post-judgment interest, costs, and disbursements as justified under 35 U.S.C. § 284;

G. And, if necessary, to adequately compensate Plaintiff for Defendant's infringement, an accounting:

i. that this case be declared exceptional within the meaning of 35 U.S.C. § 285 and that Plaintiff be awarded its reasonable attorneys’ fees against Defendant that it incurs in prosecuting this action;

ii. that Plaintiff be awarded costs, and expenses that it incurs in prosecuting this action; and

iii. that Plaintiff be awarded such further relief at law or in equity as the Court deems just and proper.

Dated: January 27, 2023

Respectfully submitted,

SAND, SEBOLT & WERNOW CO., LPA

/s/ Andrew S. Curfman

Andrew S. Curfman (SBN 0090997)
Aegis Tower – Suite 1100
4940 Munson Street NW
Canton, Ohio 44718
Telephone: (330) 244-1174
Facsimile: (330) 244-1173
Email: andrew.curfman@sswip.com

ATTORNEY FOR PLAINTIFF